Math 25: Solutions to Homework #6

(7.1 # 38) Show that $(f * g) * h = f * (g * h)$, where f and g are arithmetic functions.

For any integer n we have

$$\begin{aligned}
((f * g) * h)(n) &= \sum_{d|n} (f * g)(d) h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \left(\sum_{a|d} f(a) g\left(\frac{d}{a}\right) \right) h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \left(\sum_{ab=d} f(a) g(b) \right) h\left(\frac{n}{d}\right) \\
&= \sum_{abc=n} f(a) g(b) h(c) \\
&= \sum_{abc=n} f(a) \sum_{bc=\frac{n}{a}} g(b) h(c) \\
&= \sum_{a|n} f(a) (g * h)\left(\frac{n}{a}\right) \\
&= f * (g * h)(n)
\end{aligned}$$

(7.4 # 10) Show that if n is a positive integer, then $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

We know that in any four consecutive integers, one is divisible by four. That is, $4|(n+a)$ for some $a = 0, 1, 2, 3$. Thus $(n+a) = 2^k m$ with m odd and $k \geq 2$, so $\mu(n+a) = \mu(2^k)\mu(m) = 0$ since $\mu(2^k) = 0$ for all $k > 1$.

(7.4 # 22) Let n be a positive integer. Show that

$$\prod_{d|n} \mu(d) = \begin{cases} -1 & \text{if } n \text{ is a prime;} \\ 0 & \text{if } n \text{ has a square factor;} \\ 1 & \text{if } n \text{ is square free and composite} \end{cases}$$

We will use the fact that

$$\sum_{\substack{j=0 \\ j \text{ odd}}}^{k} \binom{k}{j}$$

is even. Let this sum be denoted a.

Now, if $n = p$ is a prime, then $\prod_{d|p} \mu(d) = \mu(1)\mu(p) = -1$.

If $s|n$ with s square, then $p^2|n$ for some prime p and $\mu(p^2) = 0$. Thus $\prod_{d|n} \mu(d) = 0$.

Finally, if n is squarefree, then $n = p_1 p_2 \cdots p_k$ and each divisor d of n is 1 or a product of distinct primes. Since $\mu(d) = (-1)^t$ where $t \leq k$ is the number of prime divisors of d, we have

$$\begin{aligned}\prod_{d|n} \mu(d) &= (-1)^k (1)^{\binom{k}{2}} (-1)^{\binom{k}{3}} (1)^{\binom{k}{4}} \cdots (\pm 1)^{\binom{k}{k}} \\ &= (-1)^a \\ &= 1,\end{aligned}$$

as a is even.

(7.4 # 30) Show that $\Sigma_{d|n} \Lambda(d) = \log n$ whenever n is a positive integer.

Recall the definition

$$\Lambda(n) = \begin{cases} \log p & n = p^k \\ 0 & \text{otherwise.} \end{cases}$$

Then if $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ is any positive integer,

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{p^k|n} \log(p) \\ &= a_1 \log(p_1) + a_2 \log(p_2) + \cdots + a_t \log(p_t) \\ &= \log(p_1^{a_1}) + \log(p_2^{a_2}) + \cdots + \log(p_t^{a_t}) \\ &= \log(n).\end{aligned}$$

(8.1 # 6) Decrypt the message RTOLK TOIK, which was encrypted using the affine transformation $C \equiv 3P + 24 \pmod{26}$.

First note that the inverse of three modulo 26 is 9, as $3 \cdot 9 = 27 \equiv 1 \pmod{26}$. Thus we have $C - 24 \equiv 3P \pmod{26}$ and $P \equiv 9(C - 24) \equiv 9(C + 2) \equiv 9C + 18 \pmod{26}$. Using this equation we arrive at the plaintext "Phone Home".

(8.1 # 8) The message KYVMR CLVFW KYVBV PZJJV MVEKV VE was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use the frequencies of letters to determine the value of k. What is the plaintext message?

The first thing to note is that the most frequently occurring letters in the ciphertext are V, with eight occurrences, and K, with three. None of the other letters occur more than twice. So it is reasonable to think that E is mapped to V and T is mapped to K under this transformation. That is, $(4 \to 21)$ and $(19 \to 10)$. Plugging either of these into the given equation $C \equiv P + k \pmod{26}$ gives a value of 17 for k. Using this we decrypt the ciphertext to: THE VALUE OF THE KEY IS SEVENTEEN.

(8.1 # 10) If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \pmod{26}$, are X and Q, respectively, then what are the most likely values for a and b?

Since the two most commonly occurring letters are X and Q, we theorize that the letter E is mapped to X and that T is mapped to Q. That is $4 \to 23$ and $19 \to 16$. Thus we consider the equations

$$23 \equiv 4a + b \pmod{26},$$

and

$$16 \equiv 19a + b \pmod{26}.$$

Subtracting these two equations yields $11a \equiv 7 \pmod{26}$. Since the inverse of 11 is 19 modulo 26, we arrive at $a \equiv 3 \pmod{26}$ and then easily find that $b \equiv 11 \pmod{26}$. Thus the affine cipher in question is $C \equiv 3P + 11 \pmod{26}$.

(8.2 # 6) Cryptanalyze the given ciphertext, which was encrypted using a Vigenère cipher.

A search for repeated triples yields three: UCY, HFT and UVB, which are separated by distances of 9, 21, and 15 letters. This suggests that the keyword length is $(9, 21, 15) = 3$. Calculating the index of coincidence (IC) for the three subsets of the ciphertext formed by taking every third letter, we have ICs of 0.0766, 0.0814, and 0.07575. Since these are near 0.065, we have the correct keyword length. Now by performing letter frequency analysis on each of the three subsets, we find that the most frequent letters in the three sets are U, C and B. After trying different possible decodings of these letters based on the most frequently used letters in the English language, we find that the correct keyword is BOX. Using this to decrypt the message, we get, "To be or not to be, that is the question. Tis' nobler in the mind to suffer the slings and arrows of outrageous fortune." Note that there is a typo in the ciphertext: the block BNKWE in the third line should be BNWKE.

(8.2 # 18(a)) How many pairs of letters remain unchanged when encryption is performed using the digraphic cipher

$$C_1 \equiv 4P_1 + 5P_2 \pmod{26}$$
$$C_2 \equiv 3P_1 + P_2 \pmod{26}.$$

We need to find letters P_1 and P_2 such that $P_1 \equiv 4P_1 + 5P_2 \pmod{26}$ and $P_2 \equiv 3P_1 + P_2 \pmod{26}$. The first congruence gives us $3P_1 + 5P_2 \equiv 0 \pmod{26}$ while the second gives $3P_1 \equiv 0 \pmod{26}$. Thus the second congruence gives $P_1 \equiv 0 \pmod{26}$ and, using this information in the first, we see that $P_2 \equiv 0 \pmod{26}$ as well. Thus the only pair of letters that is unchanged under the encryption is AA.